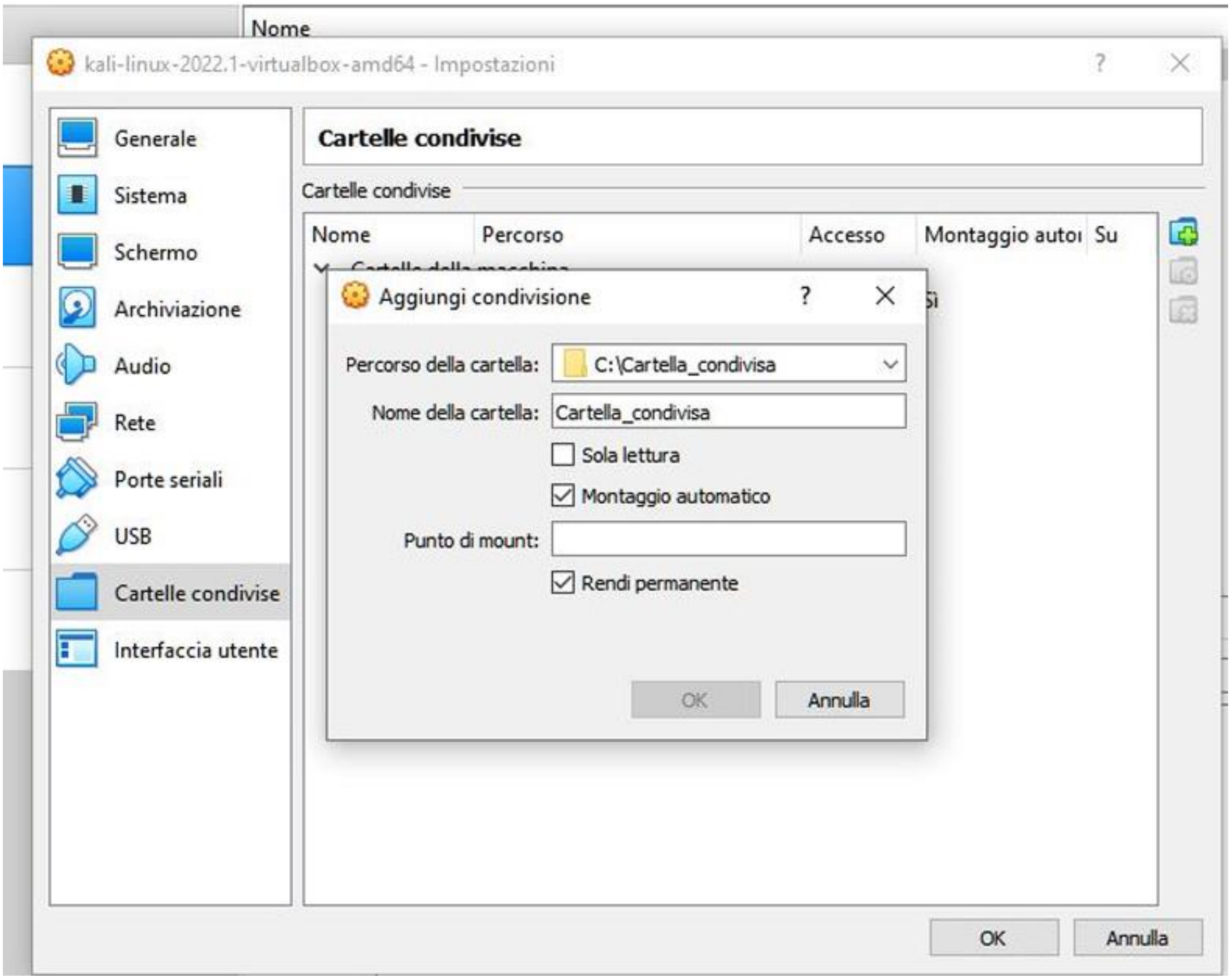
Threat Intelligence & IOC

Soluzione

Per fornire una spiegazione approfondita degli indicatori di compromissione (IOC) e degli attacchi identificati negli screenshot, analizziamo le immagini in dettaglio. Useremo le informazioni contenute in ogni screenshot per identificare le prove di attacchi e discuterne le implicazioni.

Screenshot 1: Configurazione della Cartella Condivisa



Percorso della cartella: C:\Cartella_condivisa

Nome della cartella: Cartella_condivisa

☐ Sola lettura

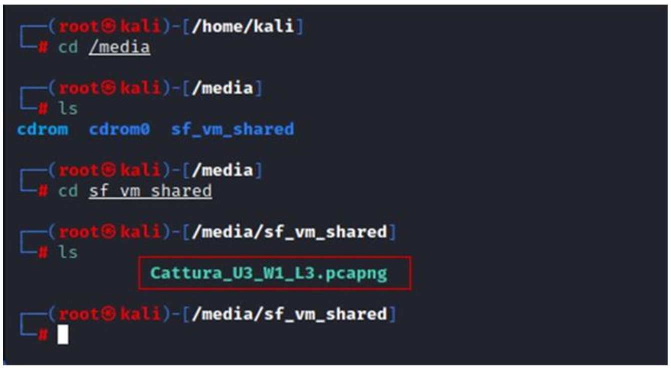
☑ Montaggio automatico

Punto di mount:

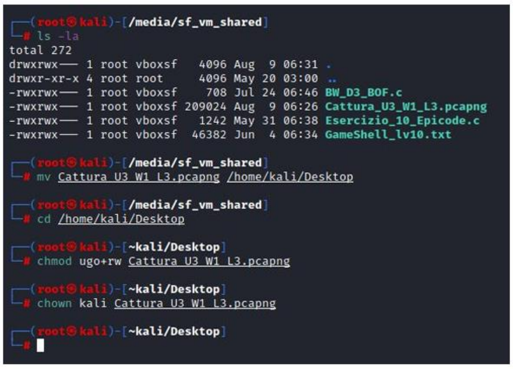
☑ Rendi permanente

Questa immagine mostra come configurare una cartella condivisa tra il sistema host e la macchina virtuale Kali Linux. Questo passaggio è necessario per trasferire il file di cattura di rete sulla macchina virtuale per l'analisi con Wireshark.

Screenshot 2: Navigazione nel File System di Kali Linux



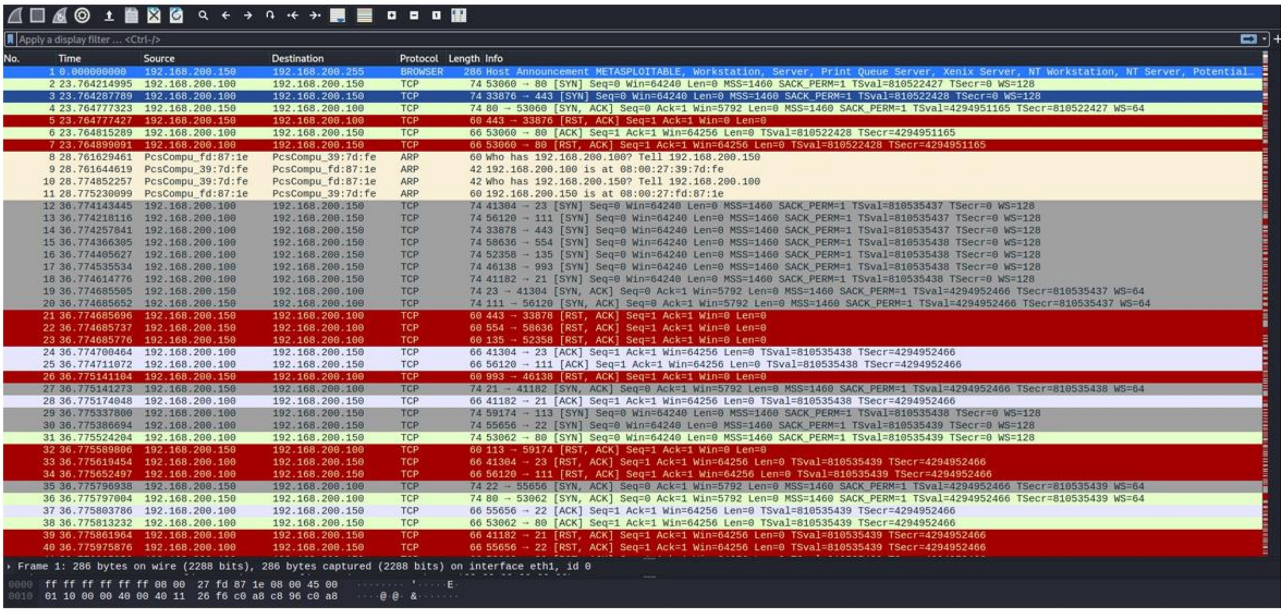
```
┌──(root㉿kali)-[/home/kali]
└─# cd /media

┌──(root㉿kali)-[/media]
└─# ls
cdrom  cdrom0  sf_vm_shared

┌──(root㉿kali)-[/media]
└─# cd sf_vm_shared

┌──(root㉿kali)-[/media/sf_vm_shared]
└─# ls
          Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[/media/sf_vm_shared]
└─# █
```



```
┌──(root㉿kali)-[/media/sf_vm_shared]
└─# ls -la
total 272
drwxrwx--- 1 root vboxsf   4096 Aug  9 06:31 .
drwxr-xr-x 4 root root     4096 May 20 03:00 ..
-rwxrwx--- 1 root vboxsf    708 Jul 24 06:46 BW_D3_BOF.c
-rwxrwx--- 1 root vboxsf 209024 Aug  9 06:26 Cattura_U3_W1_L3.pcapng
-rwxrwx--- 1 root vboxsf   1242 May 31 06:38 Esercizio_10_Epicode.c
-rwxrwx--- 1 root vboxsf  46382 Jun  4 06:34 GameShell_lv10.txt

┌──(root㉿kali)-[/media/sf_vm_shared]
└─# mv Cattura_U3_W1_L3.pcapng /home/kali/Desktop

┌──(root㉿kali)-[/media/sf_vm_shared]
└─# cd /home/kali/Desktop

┌──(root㉿kali)-[~kali/Desktop]
└─# chmod ugo+rw Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[~kali/Desktop]
└─# chown kali Cattura_U3_W1_L3.pcapng

┌──(root㉿kali)-[~kali/Desktop]
└─# █
```

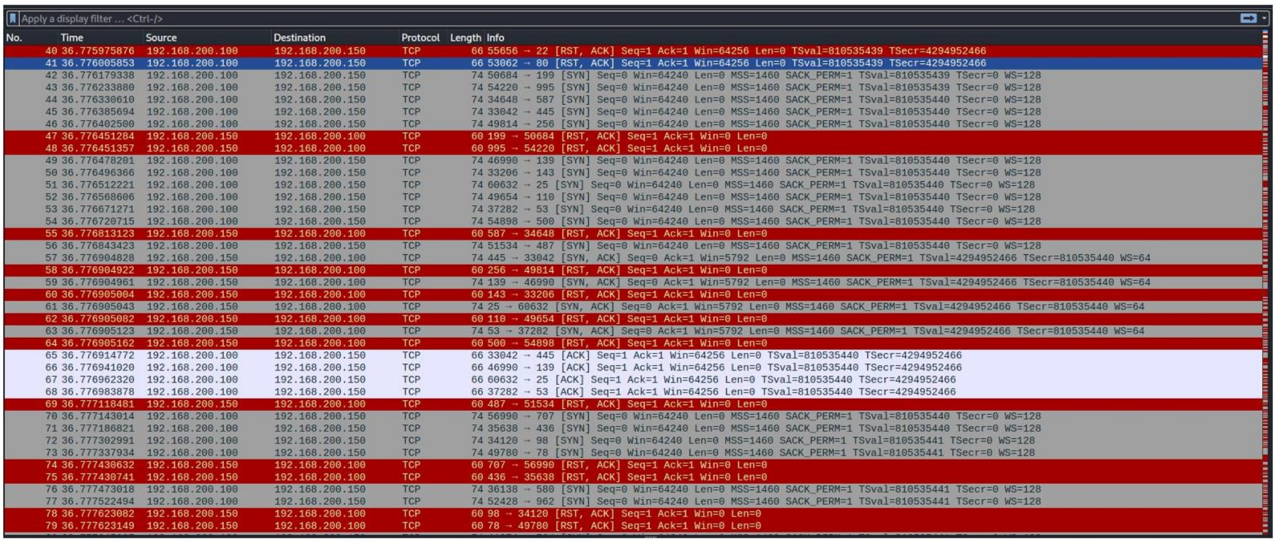
Questa immagine mostra i comandi usati per navigare nel file system di Kali Linux e spostare il file di cattura di rete sul desktop per una più facile analisi con Wireshark.

Screenshot 3-7: Analisi con Wireshark

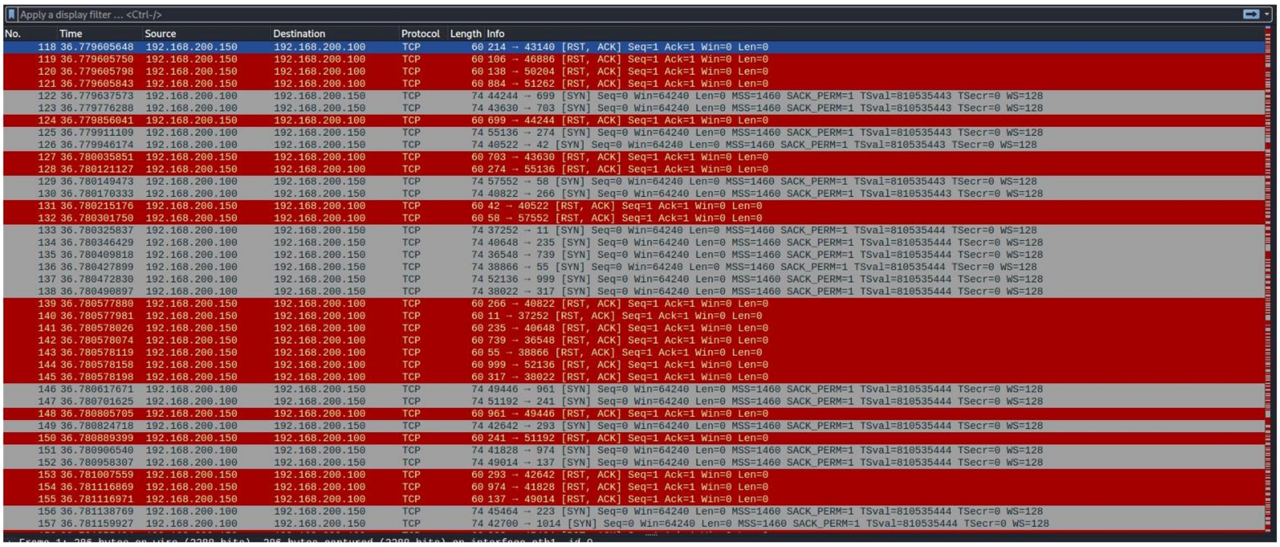


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential…
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
8	28.761629461	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PcsCompu_39:7d:fe	PcsCompu_fd:87:1e	ARP	42	Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PcsCompu_fd:87:1e	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:fd:87:1e
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466

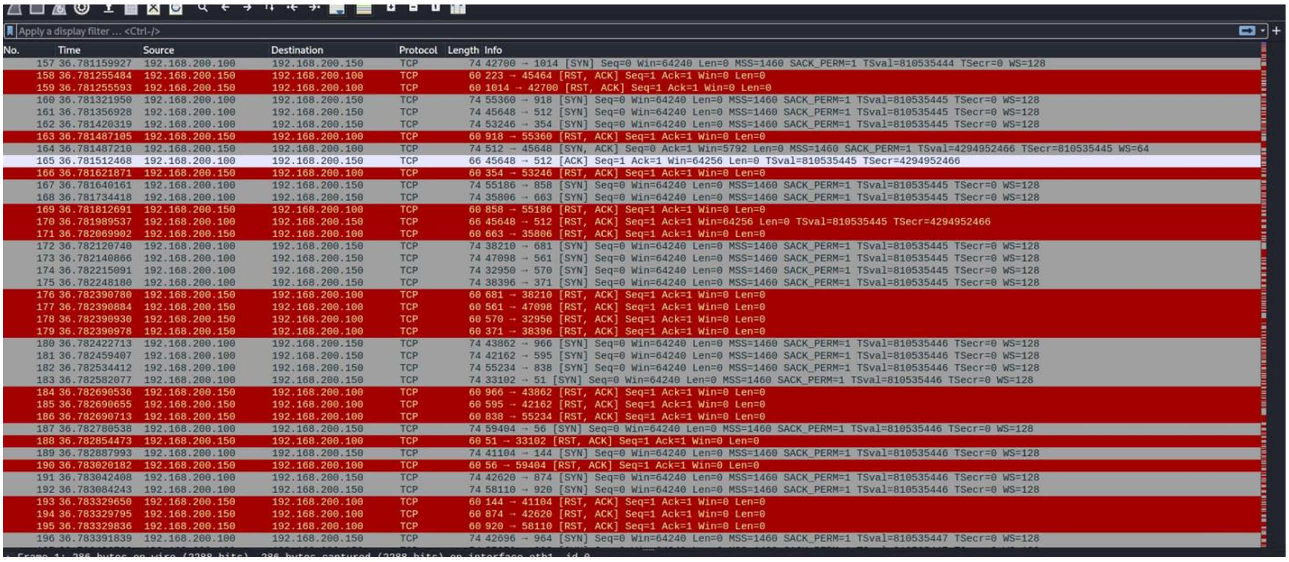
```
› Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0

0000  ff ff ff ff ff ff 08 00  27 fd 87 1e 08 00 45 00   ········'·····E·
0010  01 10 00 00 40 00 40 11  26 f6 c0 a8 c8 96 c0 a8   ····@·@·&·······
```



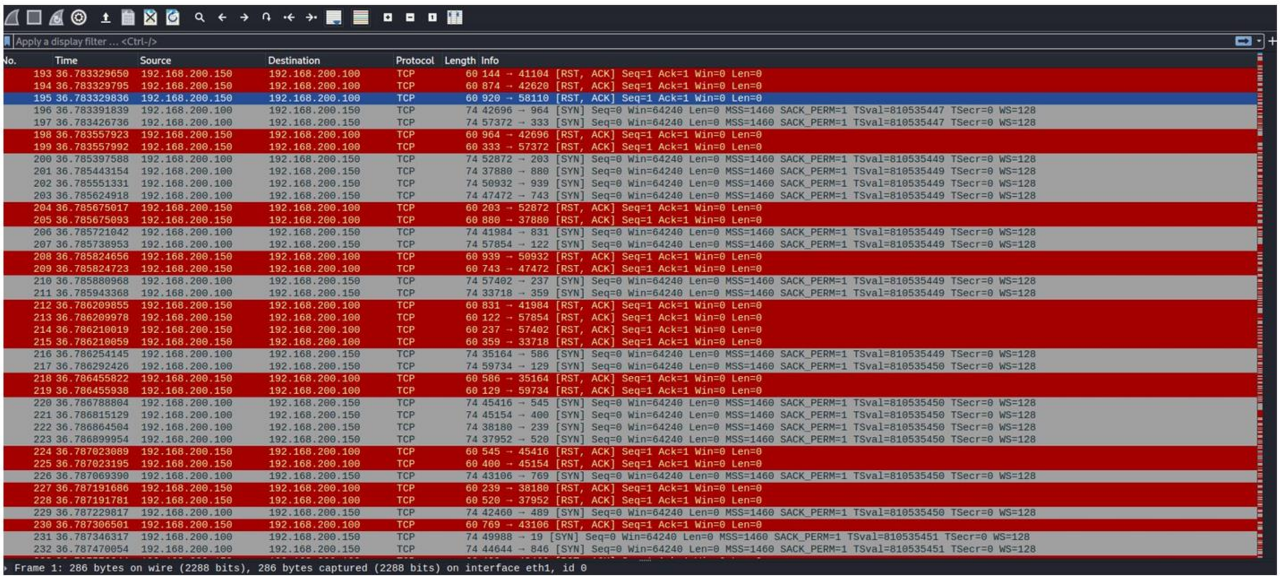
No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776478201	192.168.200.100	192.168.200.150	TCP	74	46990 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
52	36.776568606	192.168.200.100	192.168.200.150	TCP	74	49654 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776843423	192.168.200.100	192.168.200.150	TCP	74	51534 → 487 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904961	192.168.200.150	192.168.200.100	TCP	74	139 → 46990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
62	36.776905082	192.168.200.150	192.168.200.100	TCP	60	110 → 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535440 WS=64
64	36.776905162	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776914772	192.168.200.100	192.168.200.150	TCP	66	33042 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
66	36.776941020	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	66	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143014	192.168.200.100	192.168.200.150	TCP	74	56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
72	36.777302991	192.168.200.100	192.168.200.150	TCP	74	34120 → 98 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49780 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74	36.777430632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777430741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473018	192.168.200.100	192.168.200.150	TCP	74	36138 → 580 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 → 962 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623082	192.168.200.150	192.168.200.100	TCP	60	98 → 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



```
Apply a display filter ... <Ctrl-/>
No.   Time          Source           Destination      Protocol Length Info
  118 36.779605648  192.168.200.150  192.168.200.100  TCP      60 214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  119 36.779605750  192.168.200.150  192.168.200.100  TCP      60 106 → 46886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  120 36.779605798  192.168.200.150  192.168.200.100  TCP      60 138 → 50204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  121 36.779605843  192.168.200.150  192.168.200.100  TCP      60 884 → 51262 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  122 36.779637573  192.168.200.100  192.168.200.150  TCP      74 44244 → 699 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
  123 36.779776288  192.168.200.100  192.168.200.150  TCP      74 43630 → 703 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
  124 36.779856041  192.168.200.150  192.168.200.100  TCP      60 699 → 44244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  125 36.779911109  192.168.200.100  192.168.200.150  TCP      74 55136 → 274 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
  126 36.779946174  192.168.200.100  192.168.200.150  TCP      74 40522 → 42 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
  127 36.780035851  192.168.200.150  192.168.200.100  TCP      60 703 → 43630 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  128 36.780121127  192.168.200.150  192.168.200.100  TCP      60 274 → 55136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  129 36.780149473  192.168.200.100  192.168.200.150  TCP      74 57552 → 58 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
  130 36.780170333  192.168.200.100  192.168.200.150  TCP      74 40822 → 266 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
  131 36.780215176  192.168.200.150  192.168.200.100  TCP      60 42 → 40522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  132 36.780301750  192.168.200.150  192.168.200.100  TCP      60 58 → 57552 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  133 36.780325837  192.168.200.100  192.168.200.150  TCP      74 37252 → 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  134 36.780346429  192.168.200.100  192.168.200.150  TCP      74 40648 → 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  135 36.780409818  192.168.200.100  192.168.200.150  TCP      74 36548 → 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  136 36.780427899  192.168.200.100  192.168.200.150  TCP      74 38866 → 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  137 36.780472830  192.168.200.100  192.168.200.150  TCP      74 52136 → 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  138 36.780490897  192.168.200.100  192.168.200.150  TCP      74 38022 → 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  139 36.780577880  192.168.200.150  192.168.200.100  TCP      60 266 → 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  140 36.780577981  192.168.200.150  192.168.200.100  TCP      60 11 → 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  141 36.780578026  192.168.200.150  192.168.200.100  TCP      60 235 → 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  142 36.780578074  192.168.200.150  192.168.200.100  TCP      60 739 → 36548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  143 36.780578119  192.168.200.150  192.168.200.100  TCP      60 55 → 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  144 36.780578158  192.168.200.150  192.168.200.100  TCP      60 999 → 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  145 36.780578198  192.168.200.150  192.168.200.100  TCP      60 317 → 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  146 36.780617671  192.168.200.100  192.168.200.150  TCP      74 49446 → 961 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  147 36.780701625  192.168.200.100  192.168.200.150  TCP      74 51192 → 241 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  148 36.780805705  192.168.200.150  192.168.200.100  TCP      60 961 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  149 36.780824718  192.168.200.100  192.168.200.150  TCP      74 42642 → 293 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  150 36.780889399  192.168.200.150  192.168.200.100  TCP      60 241 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  151 36.780906540  192.168.200.100  192.168.200.150  TCP      74 41828 → 974 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  152 36.780958307  192.168.200.100  192.168.200.150  TCP      74 49014 → 137 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  153 36.781007559  192.168.200.150  192.168.200.100  TCP      60 293 → 42642 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  154 36.781116869  192.168.200.150  192.168.200.100  TCP      60 974 → 41828 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  155 36.781116971  192.168.200.150  192.168.200.100  TCP      60 137 → 49014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  156 36.781138769  192.168.200.100  192.168.200.150  TCP      74 45464 → 223 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  157 36.781159927  192.168.200.100  192.168.200.150  TCP      74 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
› Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
```



```
Apply a display filter ... <Ctrl-/>
No.   Time          Source           Destination      Protocol Length Info
  157 36.781159927  192.168.200.100  192.168.200.150  TCP      74 42700 → 1014 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535444 TSecr=0 WS=128
  158 36.781255484  192.168.200.150  192.168.200.100  TCP      60 223 → 45464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  159 36.781255593  192.168.200.150  192.168.200.100  TCP      60 1014 → 42700 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  160 36.781321950  192.168.200.100  192.168.200.150  TCP      74 55360 → 918 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  161 36.781356928  192.168.200.100  192.168.200.150  TCP      74 45648 → 512 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  162 36.781420319  192.168.200.100  192.168.200.150  TCP      74 53246 → 354 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  163 36.781487105  192.168.200.150  192.168.200.100  TCP      60 918 → 55360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  164 36.781487210  192.168.200.150  192.168.200.100  TCP      74 512 → 45648 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=4294952466 TSecr=810535445 WS=64
  165 36.781512468  192.168.200.100  192.168.200.150  TCP      66 45648 → 512 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
  166 36.781621871  192.168.200.150  192.168.200.100  TCP      60 354 → 53246 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  167 36.781640161  192.168.200.100  192.168.200.150  TCP      74 55186 → 858 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  168 36.781734418  192.168.200.100  192.168.200.150  TCP      74 35806 → 663 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  169 36.781812691  192.168.200.150  192.168.200.100  TCP      60 858 → 55186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  170 36.781989537  192.168.200.100  192.168.200.150  TCP      66 45648 → 512 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535445 TSecr=4294952466
  171 36.782069902  192.168.200.150  192.168.200.100  TCP      60 663 → 35806 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  172 36.782120740  192.168.200.100  192.168.200.150  TCP      74 38210 → 681 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  173 36.782140866  192.168.200.100  192.168.200.150  TCP      74 47098 → 561 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  174 36.782215091  192.168.200.100  192.168.200.150  TCP      74 32950 → 570 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  175 36.782248180  192.168.200.100  192.168.200.150  TCP      74 38396 → 371 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535445 TSecr=0 WS=128
  176 36.782390780  192.168.200.150  192.168.200.100  TCP      60 681 → 38210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  177 36.782390884  192.168.200.150  192.168.200.100  TCP      60 561 → 47098 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  178 36.782390930  192.168.200.150  192.168.200.100  TCP      60 570 → 32950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  179 36.782390978  192.168.200.150  192.168.200.100  TCP      60 371 → 38396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  180 36.782422713  192.168.200.100  192.168.200.150  TCP      74 43862 → 966 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  181 36.782459407  192.168.200.100  192.168.200.150  TCP      74 42162 → 595 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  182 36.782534412  192.168.200.100  192.168.200.150  TCP      74 55234 → 838 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  183 36.782582077  192.168.200.100  192.168.200.150  TCP      74 33102 → 51 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  184 36.782690536  192.168.200.150  192.168.200.100  TCP      60 966 → 43862 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  185 36.782690655  192.168.200.150  192.168.200.100  TCP      60 595 → 42162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  186 36.782690713  192.168.200.150  192.168.200.100  TCP      60 838 → 55234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  187 36.782780538  192.168.200.100  192.168.200.150  TCP      74 59404 → 56 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  188 36.782854473  192.168.200.150  192.168.200.100  TCP      60 51 → 33102 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  189 36.782887993  192.168.200.100  192.168.200.150  TCP      74 41104 → 144 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  190 36.783020182  192.168.200.150  192.168.200.100  TCP      60 56 → 59404 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  191 36.783042408  192.168.200.100  192.168.200.150  TCP      74 42620 → 874 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  192 36.783084243  192.168.200.100  192.168.200.150  TCP      74 58110 → 920 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535446 TSecr=0 WS=128
  193 36.783329650  192.168.200.150  192.168.200.100  TCP      60 144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  194 36.783329795  192.168.200.150  192.168.200.100  TCP      60 874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  195 36.783329836  192.168.200.150  192.168.200.100  TCP      60 920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  196 36.783391839  192.168.200.100  192.168.200.150  TCP      74 42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128
› Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
```



```
Apply a display filter ... <Ctrl-/>
No.   Time          Source           Destination      Protocol Length Info
  193 36.783329650  192.168.200.150  192.168.200.100  TCP      60 144 → 41104 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  194 36.783329795  192.168.200.150  192.168.200.100  TCP      60 874 → 42620 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  195 36.783329836  192.168.200.150  192.168.200.100  TCP      60 920 → 58110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  196 36.783391839  192.168.200.100  192.168.200.150  TCP      74 42696 → 964 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128
  197 36.783426736  192.168.200.100  192.168.200.150  TCP      74 57372 → 333 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535447 TSecr=0 WS=128
  198 36.783557923  192.168.200.150  192.168.200.100  TCP      60 964 → 42696 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  199 36.783557992  192.168.200.150  192.168.200.100  TCP      60 333 → 57372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  200 36.785397588  192.168.200.100  192.168.200.150  TCP      74 52872 → 203 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  201 36.785443154  192.168.200.100  192.168.200.150  TCP      74 37880 → 880 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  202 36.785551331  192.168.200.100  192.168.200.150  TCP      74 50932 → 939 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  203 36.785624918  192.168.200.100  192.168.200.150  TCP      74 47472 → 743 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  204 36.785675017  192.168.200.150  192.168.200.100  TCP      60 203 → 52872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  205 36.785675093  192.168.200.150  192.168.200.100  TCP      60 880 → 37880 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  206 36.785721042  192.168.200.100  192.168.200.150  TCP      74 41984 → 831 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  207 36.785738953  192.168.200.100  192.168.200.150  TCP      74 57854 → 122 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  208 36.785824656  192.168.200.150  192.168.200.100  TCP      60 939 → 50932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  209 36.785824723  192.168.200.150  192.168.200.100  TCP      60 743 → 47472 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  210 36.785880968  192.168.200.100  192.168.200.150  TCP      74 57402 → 237 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  211 36.785943368  192.168.200.100  192.168.200.150  TCP      74 33718 → 359 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  212 36.786209855  192.168.200.150  192.168.200.100  TCP      60 831 → 41984 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  213 36.786209978  192.168.200.150  192.168.200.100  TCP      60 122 → 57854 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  214 36.786210019  192.168.200.150  192.168.200.100  TCP      60 237 → 57402 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  215 36.786210059  192.168.200.150  192.168.200.100  TCP      60 359 → 33718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  216 36.786254145  192.168.200.100  192.168.200.150  TCP      74 35164 → 586 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535449 TSecr=0 WS=128
  217 36.786292426  192.168.200.100  192.168.200.150  TCP      74 59734 → 129 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  218 36.786455822  192.168.200.150  192.168.200.100  TCP      60 586 → 35164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  219 36.786455938  192.168.200.150  192.168.200.100  TCP      60 129 → 59734 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  220 36.786788804  192.168.200.100  192.168.200.150  TCP      74 45416 → 545 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  221 36.786815129  192.168.200.100  192.168.200.150  TCP      74 45154 → 400 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  222 36.786864504  192.168.200.100  192.168.200.150  TCP      74 38180 → 239 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  223 36.786899954  192.168.200.100  192.168.200.150  TCP      74 37952 → 520 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  224 36.787023089  192.168.200.150  192.168.200.100  TCP      60 545 → 45416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  225 36.787023195  192.168.200.150  192.168.200.100  TCP      60 400 → 45154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  226 36.787069390  192.168.200.100  192.168.200.150  TCP      74 43106 → 769 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  227 36.787191686  192.168.200.150  192.168.200.100  TCP      60 239 → 38180 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  228 36.787191781  192.168.200.150  192.168.200.100  TCP      60 520 → 37952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  229 36.787229817  192.168.200.100  192.168.200.150  TCP      74 42460 → 489 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535450 TSecr=0 WS=128
  230 36.787306501  192.168.200.150  192.168.200.100  TCP      60 769 → 43106 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  231 36.787346317  192.168.200.100  192.168.200.150  TCP      74 49988 → 19 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128
  232 36.787470054  192.168.200.100  192.168.200.150  TCP      74 44644 → 846 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535451 TSecr=0 WS=128
› Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0
```

Queste immagini mostrano la cattura di rete analizzata con Wireshark. Osserviamo i seguenti dettagli rilevanti:

1. **Connessioni SYN/ACK e RST**:
   - In più punti della cattura di rete, ci sono connessioni che mostrano pacchetti SYN/ACK seguiti da RST. Questo può indicare un tentativo di esaurire le risorse del server con richieste incomplete, tipico degli attacchi SYN flood.
2. **Indirizzi IP e Porte**:
   - Notiamo molteplici connessioni da e verso gli indirizzi IP `192.168.200.150` e `192.168.200.100`, utilizzando porte comuni come 80 (HTTP), 443 (HTTPS) e 445 (SMB). Questo può suggerire tentativi di sfruttamento di vulnerabilità su questi servizi.
3. **Protocolli e Lunghezze dei Pacchetti**:
   - La presenza di pacchetti con protocolli TCP, e la lunghezza variabile dei pacchetti, può fornire ulteriori indizi sulla natura del traffico di rete. Ad esempio, pacchetti SYN molto piccoli rispetto ai pacchetti di dati possono indicare scansioni delle porte.

Conclusioni

Dall'analisi delle immagini, possiamo identificare i seguenti IOC:

- **Connessioni SYN/ACK e RST ripetute**: Indicative di un potenziale attacco SYN flood.
- **Traffico su porte comuni per attacchi**: Porta 80, 443 e 445.
- **Indirizzi IP sospetti**: Specifici indirizzi IP che mostrano un comportamento anomalo.

Raccomandazioni per la Mitigazione

1. **Implementare rate limiting**: Configurare firewall per limitare il numero di richieste SYN da un singolo IP.
2. **Bloccare IP sospetti**: Utilizzare IDS/IPS per monitorare e bloccare traffico sospetto.
3. **Aggiornare sistemi e applicazioni**: Mantenere tutti i software aggiornati con le ultime patch di sicurezza.

Queste misure aiuteranno a ridurre l'impatto degli attacchi identificati e a migliorare la sicurezza della rete.